CLAIMS

What is claimed is:

1. A method comprising:

calculating a cryptogram based upon security information; and

writing the cryptogram on a magnetic stripe of a personal transaction card after a user takes possession of the card.

2. The method of claim 1, further comprising reading the security information from the magnetic stripe of the personal transaction card.

3. The method of claim 1, further comprising verifying the cryptogram by comparing it against a cryptogram generated by an independent cryptogram verification source (ICVS).

4. The method of claim 3, further comprising authorizing a transaction based upon the verifying of the cryptogram.

5. The method of claim 3, wherein the independent cryptogram verification source is a transaction privacy clearing house (TPCH).

6. The method of claim 1, wherein the security information is selected from the group consisting of:

a biometric information;

an existing data on the magnetic stripe;

a transaction amount; and

a personal identification number (PIN) code.

7. The method of claim 1, further comprising communicating with a transaction privacy clearing house (TPCH), to authorize a transaction without revealing the user's identity.

8. A method comprising:

reading security information from a magnetic stripe of a personal transaction card when the card is swiped through a device;

calculating a cryptogram using the security information;

writing the cryptogram to the magnetic stripe of the card with the device after a user takes possession of the card; and

authorizing a purchase upon verification of the cryptogram by an independent cryptogram verification source upon reading of the card at a transaction terminal.

9. The method of claim 8, further comprising authorizing access to the device by a security device.

10. The method of claim 8, wherein the independent cryptogram verification source is a transaction privacy clearing house (TPCH).

11. The method of claim 8, further comprising:

verifying that the cryptogram has been written to the card; and

receiving the card in the device for at least one additional swipe to read the data and write the cryptogram to the card if the verification fails.

12. The method of claim 8, further comprising:

sending a confirmation message to a display of the device to verify that the cryptogram has been written to the card.

13. The method of claim 8, wherein the transaction terminal is a point of sale terminal.

14. The method of claim 8, further comprising communicating with a transaction privacy clearing house (TPCH) to authorize a transaction without revealing the user's identity.

15. An apparatus comprising:

a device to calculate a cryptogram based upon a security information; and

a writer, coupled to the device, to write the cryptogram on a magnetic stripe of a personal transaction card after a user takes possession of the card.

16. The apparatus of claim 15, further comprising a secure processing unit coupled to the device to calculate the cryptogram.

17. The apparatus of claim 15, wherein the cryptogram is further based upon a current time.

18. The apparatus of claim 17, further comprising a secure time source coupled to the device to provide the current time.

19. The apparatus of claim 17, further comprising an interface with a secure time source coupled to the device to provide the current time.

20. The apparatus of claim 15, wherein the device is a personal transaction device.

21. The apparatus of claim 15, wherein the device is a hand-held, portable device.

22. The apparatus of claim 15, further comprising a reader coupled to the device to read existing data from the magnetic stripe.

23. The apparatus of claim 22, wherein the reader is built into the writer.

24. The apparatus of claim 15, further comprising a voiding component coupled to the device to void the cryptogram after the expiration of some time period.

25. The apparatus of claim 15, wherein the writer is externally located from the device.

26. The apparatus of claim 15, wherein the writer places an item of transaction data on the magnetic stripe.

27. The apparatus of claim 26, wherein the transaction data is selected from the group consisting of:

a current time;

an identification (ID) of an item to purchase;

a transaction amount limit; and

a transaction type restriction.

28. The apparatus of claim 15, wherein the security information is selected from the group consisting of:

biometric information;

existing data on the magnetic stripe;

a transaction amount; and

a personal identification number (PIN) code.

29. The apparatus of claim 15, wherein the device is selected from the group consisting of:

a privacy card;

a digital wallet; and

a privacy card configured to be coupled to a digital wallet.

30. The apparatus of claim 15, further comprising a security device coupled to the device to prevent unauthorized use of the device.

31. The apparatus of claim 30, wherein the security device is selected from the group consisting of:

a biometric security component; and

a keypad for personal identification number (PIN) code input.

32. The apparatus of claim 30, wherein the security device places a restriction on use of the device, the restriction selected from the group consisting of:

a transaction amount;

a transaction type; and

a user having authorization to use the device.

33. The apparatus of claim 15, wherein the cryptogram is a cryptographic hash value of the current time and the security information.

34. The apparatus of claim 33, wherein a key is used in calculating of the cryptographic hash value.

35. The apparatus of claim 34, wherein the key is selected from the group consisting of:

a symmetric key;

a private key; and

a secret key.

36. The apparatus of claim 15, further comprising a transaction privacy clearing house (TPCH), coupled to the device when a transaction is to be performed, to authorize the transaction based upon verification of the cryptogram.

37. The apparatus of claim 36, wherein the TPCH independently computes the cryptogram and verifies the cryptogram on the card.

38. The apparatus of claim 36, wherein the TPCH is further configured to selectively couple to a financial institution.

39. The apparatus of claim 36, wherein the TPCH further comprises a financial institution.

40. The apparatus of claim 15, further comprising a transaction terminal configured to couple to the device.

41. The apparatus of claim 40, wherein the transaction terminal is selected from the group further consisting of:

a point of sale (POS) terminal;

a home computer system;

a bank automatic teller machine (ATM) terminal;

a digital television; and

a personal POS terminal.

42. The apparatus of claim 36, further comprising a transaction terminal configured to couple to the device.

43. The apparatus of claim 42, wherein the transaction terminal, the device and the TPCH are further configured to verify each other as legitimate.

44. An apparatus comprising:

a device to calculate a cryptogram based upon a security information, the device further having a device identifier that provides no apparent identification of a user authorized to use the device;

a writer, coupled to the device, to write the cryptogram on a magnetic stripe of a personal transaction card after a user takes possession of the card;

a communication logic coupled to the device configured to communicate the device identifier and the cryptogram to a system to perform a transaction, the system comprising a secure mechanism for correlating the cryptogram, device identifier and the user; and

a security logic coupled to the device configured to allow an authorized user to use the device to perform a transaction based upon verification of the cryptogram by the system.

45. The apparatus of claim 44, wherein the security logic confirms a user of the device, the security logic selected from the group consisting of:

the cryptogram;

a personal identification number (PIN) code;

a biometric information; and

a transaction amount.

46. The apparatus of claim 44, wherein the communication logic is selected from the group consisting of:

an IC card interface;

a contactless connection;

a magnetic stripe; and

a wireless connection.

47. The apparatus of claim 44, further comprising a transaction history storage area coupled to the device and configured to store transaction records.

48. The apparatus of claim 44, further comprising a financial data storage area coupled to the device and configured to store information selected from the group consisting of electronic coupons, account balances and other data used during a transaction.

49. The apparatus of claim 44, wherein the communication logic is configured to accept direct marketing information.

50. The apparatus of claim 44, further comprising a transaction privacy clearing house (TPCH), coupled to the device when a transaction is to be performed to authorize the transaction based upon verification of the cryptogram.

51. An apparatus comprising:

a computing means for calculating a cryptogram from security information;

a writing means coupled to the computing means for writing the cryptogram to a magnetic stripe of a personal transaction card after a user takes possession of the card; and

a verifying means coupled to the computing means for verifying the cryptogram at a time of a transaction.

52. The apparatus of claim 51, further comprising a reading means coupled to the writing means for reading the security information from the magnetic stripe of a personal transaction card.

53. The apparatus of claim 51, further comprising a transaction privacy clearing house (TPCH), coupled to the computing means when a transaction is to be performed to authorize a transaction based upon verification of the cryptogram.

54. A machine-readable medium having stored thereon a plurality of instructions, which if executed by a machine, cause the machine to perform a method comprising:

calculating a cryptogram based upon security information; and

writing the cryptogram on a magnetic stripe of a personal transaction card after a user takes possession of the card.

55. The machine-readable medium of claim 54, wherein the method further comprises reading the security information from the magnetic stripe of the personal transaction card.

56. The machine-readable medium of claim 54, wherein the method further comprises verifying the cryptogram by comparing it against a cryptogram generated by an independent cryptogram verification source.

57. The machine-readable medium of claim 56, wherein the method further comprises authorizing a transaction based upon the verifying of the cryptogram.

58. The machine-readable medium of claim 54, wherein the method further comprises communicating with a transaction privacy clearing house (TPCH) to authorize a transaction without revealing the user's identity.